“PET” ที่ไม่ใช่สัตว์เลี้ยง แต่เป็นเทคโนโลยีรักษาความเป็นส่วนตัวของข้อมูล

มีนาคม 2567

NECTEC

CPS & MITeam

“PET” ที่ไม่ใช่สัตว์เลี้ยง แต่เป็นเทคโนโลยีรักษาความเป็นส่วนตัวของข้อมูล

“PET” ติดอันดับเทคโนโลยีที่น่าจับตามอง

“PET” ที่ไม่ได้แปลว่าสัตว์เลี้ยงแสนดีที่คอยเฝ้าบ้านให้เรา แต่คือเทคโนโลยีที่คอยเฝ้าระแวดระวังการเก็บรักษาความเป็นส่วนตัวของข้อมูล ท่ามกลางกระแสสังคมแห่งการใช้และแชร์ข้อมูล การปกป้องความเป็นส่วนตัวของข้อมูลก็สำคัญ สองสิ่งนี้ดูจะย้อนแย้ง แต่ก็ไม่สามารถตัดขาดจากกันได้

เทคโนโลยี **“PET” มีชื่อเรียกเต็มๆ ว่า “Privacy-Enhancing Technology”** หรือ **“เทคโนโลยีคุ้มครองความเป็นส่วนตัวของข้อมูล”** ได้รับความสนใจเป็นอย่างมากในช่วงสองปีที่ผ่านมานี้ (2021 – 2023) ท่ามกลางงานวิจัยที่เริ่ม Mature จนถูกหยิบยกมาประยุกต์ใช้งานเชิงพาณิชย์ในประเทศชั้นนำทางด้านเทคโนโลยี เช่น สหรัฐอเมริกา ประเทศสหภาพยุโรป และเริ่มขยายตัวมายังฝั่งทวีปเอเชีย เช่น เกาหลีใต้ สิงคโปร์ และเวียดนาม โดย PET ถูกจัดอันดับให้ติด Top Strategic Technology Trends จากบริษัทวิจัยและให้คำปรึกษาชั้นนำระดับโลกอย่าง Gartner ทั้งปี 2021[1] และ 2022[2] สองปีซ้อน และยังถูกพูดถึงในนิตยสาร Frobe ในปี 2021[3]

นอกจากนั้น Gartner ยังตอกย้ำความโดดเด่นของ “PET” โดยได้คาดการณ์ว่าภายในปี 2568 องค์กรขนาดใหญ่ราวๆ 60% จะใช้ Privacy-Enhancing Computation (PEC) หรือ Privacy-Enhancing Cryptographic (PEC) หนึ่งใน Subset ของเทคโนโลยี PET อย่างน้อยหนึ่งเทคนิคเพื่อการวิเคราะห์ และการประมวลผลข้อมูลบนคลาวด์ สำหรับธุรกิจบริการทางการเงินที่การแลกเปลี่ยนข้อมูลข้ามองค์กรจะช่วยเพิ่มขีดความสามารถในการวิเคราะห์การฉ้อโกง ต่อต้านการฟอกเงิน และด้านข่าวกรอง เนื่องจากข้อมูลทางการเงินของลูกค้านั้นเป็นข้อมูลอ่อนไหว การแลกเปลี่ยนข้อมูลแบบเดิมๆ ไม่สามารถทำได้โดยไม่สูญเสียความเป็นส่วนตัวของข้อมูล เทคโนโลยี PET จึงเป็นความหวังที่จะเข้ามาช่วยปิดช่องว่างของปัญหานี้

[1] https://www.gartner.com/smarterwithgartner/gartner-top-strategic-technology-trends-for-2021

[2] https://www.gartner.com/en/newsroom/press-releases/2021-10-18-gartner-identifies-the-top-strategic-technology-trends-for-2022

[3] https://www.forbes.com/sites/forbestechcouncil/2021/02/19/adding-privacy-enhancing-computation-to-your-tech-stack/?sh=494da9623de5

ทำไม “PET” ถึงสำคัญกับชีวิตผู้คน

การตื่นตัวในการปกป้องความเป็นส่วนตัวของข้อมูลส่วนบุคคล ได้รับความสนใจจากทั่วโลกมากขึ้นเรื่อยๆ จากการนำข้อมูลไปใช้ในทางที่ไม่เหมาะสมคงหนีไม่พ้น ข่าวดังระดับโลกของการรั่วไหลของข้อมูลส่วนบุคคลครั้งใหญ่ของ Facebook เมื่อปี 2018 หรือ Facebook-Cambridge Analytica Data Scandal ที่มาร์ค ซัคเคอร์เบิร์ก ซีอีโอของ Facebook ต้องขึ้นให้การกับสภาครองเกรสของสหรัฐฯ เพื่อชี้แจงว่าได้นำข้อมูลของผู้ใช้ 87 ล้านคน รั่วไหล ไปสู่บริษัทเอกชนรายหนึ่งที่ชื่อเคมบริดจ์ อะนาไลติก้า (Cambridge Analytica) ซึ่งบริษัทนี้ได้นำข้อมูลนั้นไปใช้ประโยชน์ด้วยการช่วยในแคมเปญหาเสียงของ โดนัลด์ ทรัมป์ จากพรรครีพับบลิกัน ในปี 2016 จนพาทรัมป์ พลิกสถานการณ์ แซงเอาชนะฮิลลารี่ คลินตัน ตัวเต็งจากเดโมแครต ไปได้แบบสุดเซอร์ไพรส์[4] นอกจากนี้ปัจจุบันผู้คนเริ่มให้ความสนใจและเพิ่มความระมัดระวังในการให้ข้อมูลส่วนบุคคลมากขึ้น เป็นผลมาจากที่มีข่าวการรั่วไหลของข้อมูลส่วนตัวออกมาเป็นระยะ ๆ

จากปัญหาดังกล่าว จึงทำให้เริ่มมีมาตรการปกป้องความเป็นส่วนตัวของข้อมูลส่วนบุคคล โดยสหภาพยุโรป หรือ EU ได้ออกกฎหมายคุ้มครองข้อมูลส่วนบุคคล GDPR (General Data Protection Regulation) ซึ่งมีผลบังคับใช้ตั้งแต่ 25 พฤษภาคม 2561 โดยธุรกิจที่จัดเก็บข้อมูลส่วนบุคคลของพลเมืองสหภาพยุโรปจะต้องเพิ่มมาตรการปกป้องข้อมูล โดยไม่สามารถนำข้อมูลเหล่านี้ไปใช้ในเชิงพาณิชย์ได้ หากไม่ได้รับความยินยอมจากเจ้าของข้อมูล[5] ตลอดจนการตื่นตัวของการนำข้อมูลทางด้านสาธารณสุขไปใช้ประมวลผลร่วมด้วยกับ AI โดยประเทศสหรัฐอเมริกาได้ออกกฎหมายคุ้มครองข้อมูลส่วนบุคคลเกี่ยวกับด้านสาธารณะสุข HIPAA กฎหมายว่าด้วยการเคลื่อนย้ายและความรับผิดชอบในการประกันสุขภาพ (Health Insurance Portability and Accountability Act : HIPAA)[6] นอกจากนั้นประเทศอื่นๆ ก็เริ่มหันมาให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคล เช่นเดียวกับประเทศไทย ได้มีการบังคับใช้ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล หรือ PDPA (Personal Data Protection Act) ตั้งแต่วันที่ 1 มิถุนายน 2565 ซึ่งถูกกำหนดขึ้นเพื่อใช้ในการคุ้มครองข้อมูลส่วนบุคคลไม่ให้ถูกจัดเก็บหรือนำไปใช้โดยไม่ได้แจ้งให้เราทราบและ/หรือได้รับความยินยอมจากเราในฐานะเจ้าของข้อมูลก่อน[7]

การมีกฎหมายดังกล่าวทำให้ในช่วงปีที่ผ่านมา ผู้ขอรับบริการอย่างเราจึงเริ่มต้องเซ็นเอกสารยินยอมให้บริษัทนำข้อมูลส่วนบุคคลไปใช้เพื่อแลกกับบริการที่จะได้รับ หรือต้องกดปุ่มยินยอมในแอพพลิเคชั่นเพื่อแลกกับการเข้าถึงการใช้งานบนแอพพลิเคชั่นนั้นๆ อย่างไรก็ตาม การบังคับใช้กฎหมายให้ผู้ใช้บริการยินยอมส่งมอบข้อมูล หรือยินยอมให้นำข้อมูลส่วนบุคคลไปใช้ประโยชน์นั้น ไม่ต่างอะไรกับการบีบบังคับให้ผู้รับบริการต้องสูญเสียความเป็นส่วนตัวของข้อมูลไปเพื่อแลกมากับบริการนั้น ๆ ดังนั้นจะดีกว่าหรือไม่? ถ้ามีเทคโนโลยีเข้ามาช่วยให้การคุ้มครองความเป็นส่วนตัวของข้อมูล “ทำได้ทันที” ตั้งแต่ต้นทางไปถึงปลายทางโดยผู้รับบริการไม่ต้องแลกความเป็นส่วนตัวเพื่อขอรับบริการนั้น ๆ

[4] https://workpointtoday.com/cambridge-analytica/

[5] https://www.dft.go.th/th-th/DetailHotNews/ArticleId/10986/10986GDPR

[6] https://lawforasean.krisdika.go.th/File/files/กฎหมายว่าด้วยการเคลื่อนย้ายและความรับผิดชอบในการประกันสุขภาพ.pdf

[7] https://easypdpa.com/article/easypdpa-summary-what-is-pdpa

ในขณะที่ เราปฏิเสธไม่ได้ว่าการใช้เทคโนโลยีคลาวด์ และ Internet of Things (IoT) เริ่มเข้ามามีบทบาทในด้านธุรกิจอุตสาหกรรมมากยิ่งขึ้น และเป็นหัวใจหลักสนับสนุนการก้าวสู่ Industry 4.0 ภาคธุรกิจขนาดใหญ่ต่างใช้ประโยชน์และพลังการคำนวณจากคลาวด์ทั้งในเรื่องการเข้าถึงข้อมูลได้จากทุกที่ทุกเวลา และการลดภาระการดูแลเซิร์ฟเวอร์ภายในองค์กร ดังนั้น จึงหลีกเลี่ยงไม่ได้ที่จะต้องนำข้อมูลภายในองค์กรไปประมวลผลบนคลาวด์สาธารณะ แต่กลับเกิดปัญหาข่าวการรั่วไหลของข้อมูล (Data Breach) ในผู้ให้บริการคลาวด์รายใหญ่ เช่น Amazon Web Services (AWS) และ Microsoft Azure ทำให้องค์กรต่าง ๆ เริ่มเห็นความสำคัญในการปกป้องความปลอดภัยและความเป็นส่วนตัวของข้อมูลมากยิ่งขึ้น ผู้ประกอบการต่าง ๆ เริ่มแสดงความกังวลในการนำข้อมูลที่มีความอ่อนไหว (Sensitive) ของโรงงานออกไปใช้บริการคลาวด์ สาธารณะ ดังนั้นเทคโนโลยีที่มาช่วยคุ้มครองความเป็นส่วนตัวของข้อมูลจึงน่าจะเป็นทางออกที่ตอบโจทย์ต่อประเด็นปัญหาเหล่านี้

มอง “PET” แบบลงลึกเชิงเทคนิค

PET เป็นกลุ่มของเทคโนโลยีดิจิทัลที่เข้ามาช่วยคุ้มครองความเป็นส่วนตัวของข้อมูล โดยมีความโดดเด่นที่ข้อมูลจะถูกปกป้องตั้งแต่ต้นทางไปจนถึงปลายด้วยการออกแบบตั้งแต่แรก (Privacy-by-Design) โดยเป้าหมายของการนำเทคโนโลยี PET มาใช้ สามารถแบ่งได้เป็นสองกลุ่ม คือ

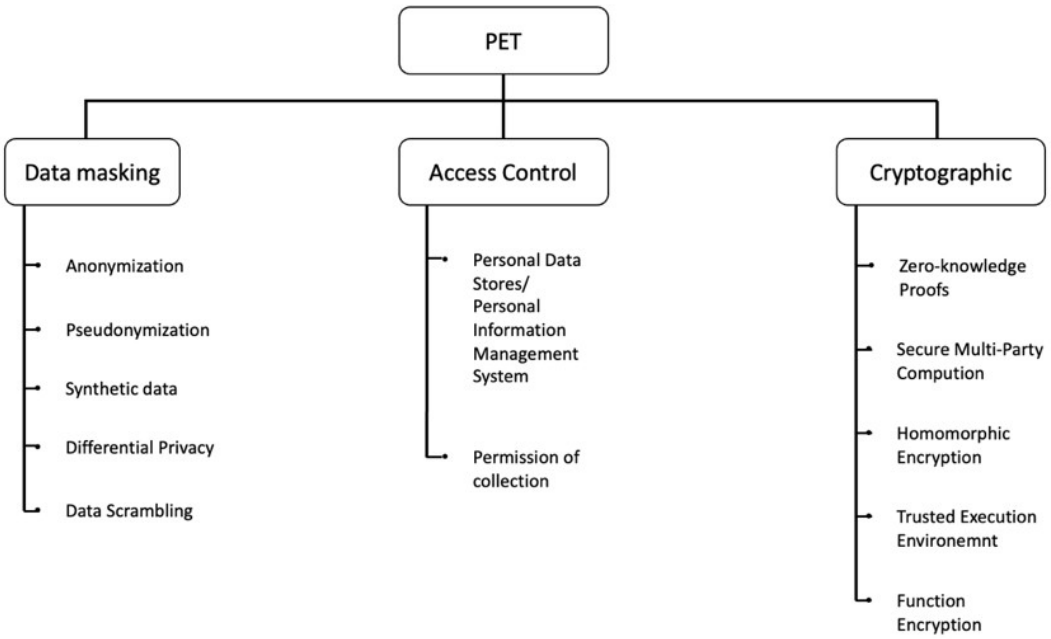
1. การปกป้องข้อมูลที่สามารถระบุตัวตนของเจ้าของข้อมูล เช่น ข้อมูลที่สามารถเชื่อมโยงความสัมพันธ์ระหว่าง ชื่อ ที่อยู่ และ เวลา ถ้าหากผู้ที่ไม่ได้รับอนุญาตให้เข้าถึงข้อมูลได้รับข้อมูลทั้งสามส่วนนี้และสามารถเชื่อมโยงถึงกันได้จะทำให้เจ้าของข้อมูลสูญเสียความเป็นส่วนตัว ดังนั้น PET จะเป็นเทคโนโลยีที่เข้ามาช่วยป้องกันความเสี่ยงนี้ โดยช่วยทำให้ข้อมูลส่วนนี้ไม่เชื่อมโยงกัน และไม่สามารถระบุตัวตนเจ้าของข้อมูลได้

2. การปกป้องการเปิดเผยข้อมูล คือการไม่เปิดเผยข้อมูลไปสู่บุคคลที่สาม โดยมุ่งเน้นไปที่การนำข้อมูลไปคำนวณบนทรัพยากรการคำนวณของบุคคลที่สาม เช่น การใช้บริการคำนวณบนคลาวด์ โดยไม่เปิดเผยข้อมูลให้กับผู้ให้บริการคลาวด์ แต่เรายังสามารถนำข้อมูลไปคำนวณและได้คำตอบ จึงเป็นสิ่งที่ท้าทายมาก โดยเทคโนโลยี PEC หนึ่งในกลุ่มเทคโนโลยี PET จะถูกนำมาใช้เพื่อป้องกันการเปิดเผยข้อมูลจริง (Data discloser) เหล่านี้

เทคโนโลยี PET สามารถแบ่งออกได้เป็น 3 กลุ่มตามเทคนิคที่นำมาใช้[8] ได้แก่

1. **Data masking** การทำ Data marking เป็นการปกปิดข้อมูลที่จะบ่งชี้ถึงสิ่งที่จะละเมิดความเป็นส่วนตัวของเจ้าของข้อมูล เช่น การนำข้อมูลที่บ่งชี้ถึงตัวตน เช่น ชื่อ ID และเลขบัตรเครดิตของลูกค้าออกจากข้อมูลที่ต้องการนำไปประมวลผลทางสถิติ
2. **Access control** เป็นเทคนิคที่พัฒนามาเพื่อปกป้องการเข้าถึงข้อมูลโดยผู้ไม่ได้รับอนุญาต เป็นเทคนิคที่ใช้ในการกำจัดสิทธิ์และตรวจสอบสิทธิ์ในการเข้าถึงข้อมูล
3. **Cryptographic** เป็นเทคนิคการใช้วิทยาการเข้ารหัสข้อมูลมาเพื่อแปลงข้อมูลให้สามารถนำข้อมูลที่ถูกแปลงแล้วไปคำนวณต่อโดยข้อมูลจริงไม่ถูกเปิดเผย

[8] https://csrc.nist.gov/projects/pec



Cryptographic คำนวณข้อมูลลับด้วยเทคนิค “PEC”

“ความลับไม่มีในโลก” อาจใช้ไม่ได้กับเทคโนโลยี PEC หรือ Privacy Enhancing Computation/ Cryptographic โดย PEC เป็นหนึ่งในกลุ่มเทคนิคที่ถูกพัฒนาขึ้นเพื่อทำให้ความลับของข้อมูลที่ถูกนำไปประมวลผลบนพื้นที่ของผู้ให้บริการคลาวด์ ยังคงเป็นความลับต่อไปโดยไม่ถูกเปิดเผย “เหมือนดั่งเวทย์มนต์” ใครจะจินตนาการได้ว่าการนำข้อมูลมาคำนวณ จะสามารถทำได้โดยผู้คำนวณนั้นไม่รู้เลยว่ากำลังคำนวณข้อมูลอะไรและมีค่าเท่าใด การจุดประกายจากโมเดลทางคณิตศาสตร์ของวิทยาการเข้ารหัสในอดีต ทำให้นักวิจัยและนักคณิตศาสตร์ในปัจจุบันต่างหันมาให้ความสนใจพัฒนาเทคโนโลยีด้วยการผสมผสานทั้งเทคนิคด้านวิทยาการเข้ารหัส โพรโตคอลการสื่อสาร และระเบียบวิธีการปกปิดข้อมูลที่บ่งชี้ถึงความอ่อนไหวของข้อมูล กลายเป็นเทคนิคใหม่ ๆ เพื่อเป็นเวทย์มนต์แห่ง PEC โดยจะกล่าวถึง 4 อันดับแรกได้แก่

1. Zero-Knowledge-Proofs (ZKP) เป็นเทคโนโลยีที่ใช้ Cryptographic protocol ในการพิสูจน์ว่าคนหนึ่ง (Prover) รู้ข้อมูลบางส่วนกับอีกคนหนึ่งซึ่งเป็นผู้ตรวจสอบ (Verifier) โดยไม่เปิดเผยข้อมูลนั้นกับผู้ตรวจสอบ เป้าหมายของ ZKP คือเพื่อโน้มน้าวให้ผู้ตรวจสอบเชื่อว่า Prover รู้ข้อมูลนั้นจริง แต่ฝ่าย Verifier จะไม่สามารถรู้ข้อมูลจริงนั้นได้ การทำเช่นนี้จะสำเร็จได้ด้วยคุณลักษณะสามประการ คือ 1) ความครบถ้วนสมบูรณ์ ซึ่งจะเกิดขึ้นเมื่อ Prover เคลมว่ารู้ข้อมูลนั้นจริงต่อฝ่าย Verifier และสามารถเคลมได้อย่างยาวนานเพียงพอที่จะพิสูจน์ได้ว่า Prover รู้ข้อมูลนั้นจริง 2) ฟังดูสมเหตุสมผล หาข้อมูลที่เคลมนั้นฟังดูไม่สมเหตุสมผลเมื่อไหร่ก็ตาม Prover จะถูกปฏิเสธความน่าเชื่อถือโดยทันที และ 3) Verifier จะไม่รู้อะไรเกี่ยวกับข้อมูลนั้นเลย

ตัวอย่างเช่น การพิสูจน์ได้ว่าบุคคลนี้มีสถานการณ์การเงินที่เพียงพอต่อการกู้ยืม โดยไม่เปิดเผยตัวเลขในบัญชีธนาคาร พิสูจน์การทำธุรกรรมทางการเงินสมบูรณ์โดยไม่เปิดเผยข้อมูลชื่อบัญชี การพิสูจน์ตัวตนของข้อมูลโดยที่ไม่เปิดเผยข้อมูล เป็นต้น ZKP อาศัยเทคนิคการทำ Hashing และโพรโตคอลสำหรับการเข้ารหัสข้อมูล ประโยชน์ในการนำ ZKP ไปใช้ ได้แก่ การช่วยทำให้การตรวจสอบ Transaction ของ Blockchain ขยายตัวได้ดีขึ้น ทำให้ลด

ข้อจำกัดของความซับซ้อนในการตรวจสอบบน Blockchain โดยการตรวจสอบ Off-chain นอกจากนี้ ZKP ยังสามารถถูกนำไปใช้ในด้าน Finance การโหวตออนไลน์ และการทำ Anonymous transaction บน Privacy coins สำหรับ Blockchain อีกด้วย

2. Secure Multiparty Computation (SMPC) เป็นเทคนิคการคำนวณแบบกระจายการคำนวณไปยังหน่วยคำนวณย่อย โดยข้อมูลที่ต้องการนำมาร่วมคำนวณจะถูกแบ่งออกเป็นส่วนๆ ตามจำนวนผู้เข้ามาร่วมช่วยคำนวณ และข้อมูลที่ถูกแบ่งเหล่านั้นจะถูกปลอมปนด้วย Noise และผู้ช่วยคำนวณทั้งหลายไม่สามารถล่วงรู้ข้อมูลจริงของผู้อื่น และไม่สามารถรู้ผลลัพธ์ของการคำนวณได้เช่นกัน เทคนิคนี้อาศัยโพรโทคอลการสื่อสารที่ออกแบบมาเฉพาะเพื่อให้การคำนวณเป็นไปอย่างปลอดภัยและเป็นความลับ และจำเป็นต้องอาศัยคนกลางทำหน้าที่ควบคุมโพรโทคอลที่ตกลงกันและคำนวณผลลัพธ์สุดท้าย วิธี SMPC นี้ เป็นการคำนวณแบบ Distributed Computing ซึ่งเริ่มถูกนำมาประยุกต์ใช้ร่วมกับ Blockchain และ Homomorphic Encryption การนำเทคโนโลยีนี้ไปใช้ร่วมกับ ZKP เพื่อทำให้ Blockchain มีประสิทธิภาพและรักษาความเป็นส่วนตัวมากยิ่งขึ้น โดย วิธี SMPC ถูกนำไปประยุกต์ใช้อย่างแพร่หลายในการคำนวณฐานเงินเดือนจาก HR หรือการตรวจสอบการโกงด้านการเงิน หรือคำนวณไฟฟ้า การขายคืนค่าไฟฟ้า เป็นต้น

3. Homomorphic Encryption (HE) เป็นเทคนิคการเข้ารหัสโดยข้อมูลที่ถูกเข้ารหัสสามารถนำไปคำนวณได้โดยไม่ต้องถอดรหัสบนสภาพแวดล้อมโฮโมมอร์ฟิก ซึ่งข้อมูลที่ถูกนำไปคำนวณบนหน่วยประมวลผลภายนอก เช่น คลาวด์สาธารณะ ไม่ถูกเปิดเผยสู่คลาวด์ การเข้ารหัสแบบโฮโมมอร์ฟิกอาศัยคุณสมบัติของ Ring Number ทำให้ข้อมูลที่ถูกเข้ารหัสนั้นเมื่อนำไปคำนวณ หรือทำโอเปอร์เรชั่นทางคณิตศาสตร์แล้วผลลัพธ์ของข้อมูลที่ถูกถอดรหัสจะได้ค่าใกล้เคียงกับการคำนวณบนข้อมูลที่ไม่เข้ารหัส ความมหัศจรรย์ทางคณิตศาสตร์ของคุณสมบัติโฮโมมอร์ฟิกนี้ทำให้นักคณิตศาตร์และนักวิจัยทั่วโลกต่างให้ความสนใจพัฒนากันต่อมา เราสามารถแบ่ง HE ได้เป็น 3 ประเภทตามคุณสมบัติของความสามารถในการคำนวณ นั่นคือ 1) PHE (Partial Homomorphic Encryption) มีคุณสมบัติในการรองรับการทำโอเปอร์เรชั่นได้เพียงอย่างใดอย่างหนึ่งระหว่างการคูณ และการบวก และไม่สามารถคำนวณต่อๆ กันได้หลายรอบ ทำให้การนำ PHE ถูกจำกัด แต่ข้อดีคือมีความซับซ้อนน้อย Overhead ต่ำ 2) SWHE (Somewhat Homomorphic Encryption) มีคุณสมบัติในการรองรับการทำโอเปอร์เรชั่นได้ทั้งบวกและคูณแต่จำนวนรอบในการคำนวณต่อๆ กันมีจำกัด มีความซับซ้อนมากกว่า PHE และ Overhead สูงกว่า PHE 3) FHE (Fully Homomorphic Encryption) คุณสมบัติในการรองรับการทำโอเปอร์เรชั่นได้ทั้งบวกและคูณ สามารถรองรับการทำโอเปอร์ชั่นได้หลากหลาย และจำนวนรอบในการคำนวณต่อๆ กันมากขึ้น แต่มีความซับซ้อนสูง และมี Overhead สูงกว่า PHE และ SWHE ทำให้การเลือกใช้ HE แต่ละวิธีต้องคำนึงถึงความเหมาะสมต่อการนำไปใช้งาน เพราะความหลากหลายของการทำโอเปอร์เรชั่นต้องแลกมากับความซับซ้อนและการใช้ทรัพยากรในการบรรจุข้อมูลสูง

อย่างไรก็ตามวิธี HE เป็นที่ดึงดูดนักวิจัยและพัฒนาให้หันมาสนใจสูงเนื่องจากเป็นวิธีที่ทำให้ความเป็นส่วนตัวของข้อมูลยังถูกคุ้มครองตั้งแต่ต้นทางถึงปลายทาง และเมื่อเกิดเหตุการณ์คลาวด์ถูกโจมตีทางไซเบอร์ข้อมูลที่ถูกนำไปคำนวณบนคลาวด์ก็ยังคงไม่รั่วไหลไปสู่บุคคลภายนอกอีกด้วย ดังนั้นนักวิจัยจึงหันมาพยายามพัฒนา HE

เพื่อลดข้อจำกัดด้านความซับซ้อนลงแต่ยังคงความปลอดภัยไว้ จนทำให้ในปัจจุบันได้มีบริษัท Startup หลายบริษัทให้บริการคำนวณด้านการธนาคาร การให้สินเชื่อกู้ยืมเงิน ด้านการแพทย์ และ HR

4. TEE (Trusted Execution Environment) หรือ Secure Enclave เป็นเทคโนโลยีที่อาศัยฮาร์ดแวร์เฉพาะในการสร้างพื้นที่ปลอดภัยที่อยู่ในหน่วยประมวลผล (CPU) ที่แม้แต่เจ้าของหน่วยประมวลผลนั้นก็ไม่สามารถเข้าถึงพื้นที่ส่วนนี้ได้ถ้าไม่ได้รับอนุญาต ซึ่งเปรียบเสมือนการสร้างถ้ำลับในเครื่องเซิร์ฟเวอร์ที่ต้องอาศัยกุญแจอีกชั้นในการเข้าถึง การนำข้อมูลที่เข้ารหัสมาเข้าไปใน Secure Enclave นี้เพื่อทำการถอดรหัสก่อนการนำข้อมูลไปประมวลผล ดังนั้นการประมวลผลจะทำบนข้อมูลจริง และภายหลังการคำนวณเสร็จสิ้น ข้อมูลจะถูกเข้ารหัสก่อนส่งออกมาจากพื้นที่ดังกล่าว การเข้ารหัสและการถอดรหัส และการคำนวณนี้กระทำบนพื้นที่ CPU เฉพาะ โดยซอฟต์แวร์และแอพพลิเคชั่นอื่น ๆ บน เครื่องเซิร์ฟเวอร์ไม่สามารถเข้าถึงได้หากปราศจากกุญแจถอดรหัส และกุญแจนี้จะมีเพียงเจ้าของข้อมูลเท่านั้นที่มี เทคโนโลยีนี้ถูกนำมาให้บริการบนคลาวด์ AWS และ Azure โดยได้เปิดให้ผู้ใช้บริการเลือกใช้ TEE สำหรับการจัดเก็บข้อมูล และการประมวลผลข้อมูลได้ แต่การเลือกใช้จะถูกผูกติดกับฮาร์ดแวร์และซอฟต์แวร์เฉพาะที่ถูกออกแบบมาเท่านั้น เช่น Intel SGX ซึ่งทำให้การเลือกใช้บริการ TEE ยังถูกจำกัด

“PET” ต่างจาก Blockchain ที่เราคุ้นเคยอย่างไร

หลายคนสงสัยว่า Blockchain เป็นเทคโนโลยีที่ช่วยแก้ปัญหาด้านความเป็นส่วนตัวหรือไม่ และเพราะเหตุใด Blockchain จึงไม่ถูกจัดให้อยู่ในกลุ่มเทคโนโลยี PET

กลับมาทำความเข้าใจก่อนว่า Blockchain นั้นเป็นเทคโนโลยีที่ถูกพัฒนาโดยมีเป้าหมายเพื่อความปลอดภัยและความโปร่งใสของการบันทึกและส่งข้อมูลในการกระจายตัวของบัญชี (Distributed ledger) แบบดิจิทัล ซึ่งถูกนำมาใช้ใน Bitcoin ครั้งแรกในปี 2008 ด้วยการอาศัยเทคนิคการทำ Hashing ข้อมูลที่ถูกบันทึกใน Blockchain ไม่สามารถเปลี่ยนแปลงได้ ทำให้การบันทึกข้อมูลลงบน Blockchain เป็นการยืนยันถึง Integrity ของข้อมูล ความตั้งใจในการพัฒนา Blockchain ให้มีคุณสมบัติ Immutability นั่นคือ ข้อมูลที่ถูกบันทึกไว้ใน Blockchain จะไม่สามารถถูกลบและเปลี่ยนแปลงได้ คุณสมบัติ Transparency หรือความโปร่งใสตรวจสอบได้ นั่นหมายถึงทุกคนที่เข้าถึง Blockchain นี้จะสามารถตรวจสอบความถูกต้องของข้อมูลได้พร้อม ๆ กัน และคุณสมบัติ Accountability ที่ทำให้ทุกคนมีส่วนรับผิดชอบต่อข้อมูลใน Blockchain เนื่องจากถูกออกแบบมาเพื่อการกระจายตัวไม่มีใครคนใดคนหนึ่งเป็นผู้รับผิดชอบ ดังนั้นด้วยคุณสมบัติของ Blockchain จึงขัดแย้งกับคุณสมบัติการปกป้องความเป็นส่วนตัวของข้อมูลโดยสิ้นเชิง ทั้งนี้เนื่องจาก Blockchain ไม่ได้มีเป้าหมายในการป้องกันความเป็นส่วนตัวของข้อมูลในการออกแบบตั้งแต่แรก

เนื่องจากกระแสความเป็นส่วนตัวของข้อมูลเริ่มมีมากขึ้น จึงทำให้มีผู้นำเอาเทคโนโลยี PET เข้ามาเป็น “ตัวช่วย” ทำให้ Blockchain สามารถป้องกันความเป็นส่วนตัวของข้อมูลได้เพิ่มขึ้นต่างหาก เช่น การทำ ZKP, SMCP และ FHE เป็นต้น

“PET” กับการใช้ประโยชน์ในนานาประเทศ

หลายประเทศชั้นนำด้านเทคโนโลยีของโลกได้นำเทคโนโลยี PET มาใช้เพื่อคุ้มครองความเป็นส่วนตัวของข้อมูล[9] เช่น ประเทศ**เยอรมันนี**ใช้ในการลดการ Tracking ผู้ใช้งานหรือผู้รับบริการ ในเรื่องการรวบรวมข้อมูล การให้การยินยอมโดยเจ้าของข้อมูลกับ Third-Party ที่ต้องการนำข้อมูลนั้นไปใช้งานต่อได้ ในขณะที่ประเทศ**ฝรั่งเศส**ใช้งานด้านการป้องกันการยิงโฆษณา และสร้างสภาพแวดล้อมความเป็นส่วนตัวในการใช้งานข้อมูลออนไลน์ ประเทศ**เนเธอร์แลนด์**เน้นการคุ้มครองความเป็นส่วนตัวของข้อมูลด้านสาธารณสุข ซึ่งคล้ายกับประเทศ**สหรัฐอเมริกา**ที่ใช้ในงานทางด้านสาธารณสุข และนอกเหนือจากนั้นทางประเทศสหรัฐอเมริกายังได้นำไปใช้กับงานด้านการทหาร การเงินการธนาคารและการประมูล ส่วนประเทศ**สวีเดน**ใช้คุ้มครองความเป็นส่วนตัวของข้อมูล Face Recognition

อย่างไรก็ตาม ด้วยคุณประโยชน์ของเทคโนโลยีนี้ ทำให้มีแนวโน้มการนำ PET ไปใช้กับงานที่เกิดผลกระทบสูงต่อความมั่นคงปลอดภัยของประเทศขยายวงกว้างในอีกหลาย ๆ ประเทศ นอกจากประเทศชั้นนำด้านเทคโนโลยีที่เริ่มมีการตื่นตัวในการเป็นผู้นำเทรนที่ได้ประยุกต์ใช้เทคโนโลยี PET ในการจัดการข้อมูลในหลายๆ มิติแล้ว ยังมีประเทศเพื่อนบ้านของเราที่ได้ให้ความสนใจที่เปิดตัวแลปวิจัยทางด้านเทคโนโลยีนี้โดยเฉพาะ ได้แก่ ประเทศเวียดนาม และประเทศสิงคโปร์ ในประเทศ**เวียดนาม** มีการก่อตั้งองค์กรวิจัยแบบไม่แสดงหาผลกำไรของนักวิจัยและพัฒนาชาวเวียดนามภายใต้ชื่อ ZKP Labs ที่พุ่งเป้าไปที่การให้ความรู้ การพัฒนา และวิจัยที่เกี่ยวข้องกับเทคโนโลยี ZKP โดยมีเป้าหมายเปรียบเสมือนบ้านของนัก Cryptography และผู้หลงใหลในการพัฒนา ZKP มารวมตัวกันจัดกิจกรรมสร้างสรรค์เพื่อพัฒนาต่อยอด ZKP ไปยังเทคโนโลยีต่างๆ เช่น Web3

สำหรับรัฐบาลประเทศ**สิงคโปร์**ได้ให้ความสำคัญในเทคโนโลยี PET โดยจัดให้มี PET Sandbox[10] ซึ่งได้รับการสนับสนุนจากหน่วยงาน the Infocomm Media Development Authority and Personal Data Protection Commission (PDPC) ทั้งนี้ทางรัฐบาลประเทศสิงคโปร์ได้กล่าวว่า PET เป็นความหวังใหม่ของธุรกิจการนำเทคโนโลยี AI ไปใช้ ซึ่งจะก่อให้เกิดประโยชน์อย่างมหาศาลกับภาคธุรกิจไม่ว่าจะเป็นการธนาคารที่การแชร์ข้อมูลข้ามธนาคารกันสามารถทำได้โดยยังสามารถปกป้องผลประโยชน์ความเป็นส่วนตัวของข้อมูลลูกค้าในขณะที่ธนาคารเองสามารถใช้ข้อมูลที่แชร์ร่วมกันข้ามองค์กรมาตรวจสอบการฟอกเงิน หรือโจรกรรมทางการเงินได้ นอกจากนั้นรัฐบาลประเทศสิงคโปร์ยังได้แสดงวิสัยทัศน์มองไปถึงการปกป้องความเป็นส่วนตัวของข้อมูลจะช่วยผลักดันให้ต้นทุนการทำธุรกิจของ Startup และบริษัทยักษ์ใหญ่มีความเหลื่อมล้ำของข้อมูลลดลง

[9] https://app.dealroom.co/lists/32718

[10] https://www.imda.gov.sg/how-we-can-help/data-innovation/privacy-enhancing-technology-sandboxes

งานวิจัยเกี่ยวกับ “PET” ของประเทศไทยและเนคเทค

จากสถานการณ์ที่ทั่วโลกเริ่มตื่นตัวตอบรับเทคโนโลยี PET และมองว่าอาจเป็นเทคโนโลยีจุดเปลี่ยนของโลกอีกเทคโนโลยีหนึ่ง ดังนั้นทำให้เราต้องย้อนกลับมามองที่ประเทศไทย และตั้งคำถามว่า “ประเทศทั่วโลกตื่นแล้ว ประเทศไทยตื่นหรือยัง?” บ่อยครั้งที่เทคโนโลยีทันสมัย มักเริ่มจากประเทศชั้นนำด้านเทคโนโลยี ส่วนไทยมักจะเป็นประเทศปลายน้ำที่นำเข้าเทคโนโลยี อีกทั้งบริษัทในไทยมักให้คุณค่ากับเทคโนโลยีนำเข้ามากกว่าการสนับสนุนเทคโนโลยีที่พัฒนาเองในประเทศ แต่ไม่ใช่กับเทคโนโลยี PET

อาจกล่าวได้ว่านักวิจัยและนักวิชาการของไทยที่เริ่มให้ความสนใจเข้ามาศึกษาวิจัยเทคโนโลยี PET มีเพียงแค่หยิบมือ เห็นได้จากผลงานวิจัยที่ตีพิมพ์ในงานประชุมวิชาการและวารสารวิชาการการระดับนานาชาติ หรือแม้กระทั่งงานวิทยานิพนธ์ก็มีไม่มากนัก โดยมีงานวิจัยได้ศึกษาเกี่ยวข้องกับ Differential Privacy[11] การศึกษาสำรวจเกี่ยวกับเทคโนโลยี FHE เป็นต้น โดยงานวิจัยเหล่านี้เป็นการศึกษาถึงการปรับปรุงและแนวทางในการนำเทคโนโลยี PET มาประยุกต์ใช้งานกับแอปพลิเคชั่นด้านการจัดการพลังงาน และด้านอื่นๆ แต่ยังไม่มีงานวิจัยที่บ่งชี้ถึงการนำเอาเทคโนโลยี PET มาพัฒนาเป็นแพลตฟอร์มที่สามารถใช้งานจริงในภาคอุตสาหกรรมได้

สำหรับเนคเทค โดย Sustainable Manufacturing Center หรือ SMC มีพันธกิจหลักในการผลักดันอุตสาหกรรมไทยไปสู่ยุค Industry 4.0 ซึ่งจำเป็นต้องใช้บริการการคำนวณบนคลาวด์ หรือแม้กระทั่งการผลักดันในภาคอุตสาหกรรมก้าวไปสู่ยุค Autonomous ไม่ว่าด้วยเทคโนโลยี AI หรือ Digital Twin มากยิ่งขึ้น แต่การขับเคลื่อนเทคโนโลยีดังกล่าวควรมีการผลักดันเทคโนโลยีด้านความปลอดภัยทางไซเบอร์และการคุ้มครองความเป็นส่วนตัวของข้อมูลด้วย ในปัจจุบัน ทีมวิจัยระบบไซเบอร์-กายภาพ (CPS) ได้พัฒนาเทคโนโลยี PET เป็น “**PET as-a-service for IoT/IIoT platform” ขึ้นภายใต้ผลงาน “ไซบีเลียน” หรือ “CYBLION”** ซึ่งมาจากการผสานสองคำ "Cyber” และ "Brilliant" ปัจจุบันมีเป้าหมายใช้สนับสนุนการทำงานในโรงงานเป็นหลัก

โดยในระบบเดิมนั้นใช้ Cloud จากภายนอก ซึ่งถูกขโมยข้อมูลส่วนบุคคลบ่อยครั้ง ฉะนั้นเราจะไว้ใจ Cloud จากภายนอกได้อย่างไรบ้าง? ทางทีมนักวิจัยจึงค้นหาแนวทางการปกป้องข้อมูลในแง่ของกฎหมายและแง่ของการใช้

[11] https://ieeexplore.ieee.org/abstract/document/9663169

งาน จึงใช้ระบบ Homomorphic Encryption (HE) คือการให้ Cloud วิเคราะห์ข้อมูลโดยไม่จำเป็นต้องให้คีย์ในการไขเปิดข้อมูลส่วนบุคคล ซึ่งจะทำให้ยังคงรักษาข้อมูลส่วนบุคคลได้ และ Cloud จะจัดการคำนวณโดยที่ไม่ต้องเปิดเผยข้อมูลส่วนบุคคลได้ด้วย ฉะนั้น CYBLION จะการันตีว่าข้อมูลส่วนบุคคลจะไม่หลุดออกจากระบบ เพราะใช้ระบบและเทคโนโลยีในการจัดการและจัดเก็บข้อมูลโดยที่ยังคงรักษาข้อมูลส่วนบุคคลให้ลูกค้าสามารถจัดการได้ด้วยตนเอง ซึ่งจะเป็นการแก้ไขปัญหาการหลุดรั่วไหลของข้อมูลส่วนบุคคลได้นั่นเอง และทำให้การคุ้มครองความเป็นส่วนตัวของข้อมูล IoT/IIoT เป็นเรื่องง่าย ๆ เพียงปลายนิ้วด้วยการเข้าถึงได้ด้วยตนเองผ่าน mobile application ที่เปิดให้ผู้ใช้ดาวน์โหลดได้ทั้ง Apple Store และ Google Play Store อีกทั้งยังให้ผู้ใช้งานสามารถสร้างฟังก์ชั่นการคำนวณบนคลาวด์ได้ด้วยตนเองอีกด้วย ทำให้ผู้ประกอบการในไทยมีความตื่นตัวและเข้าถึงเทคโนโลยีนี้ได้ง่าย **ซึ่งในปัจจุบันพบว่าแทบจะไม่มี Platform ใด ที่สร้างมาเพื่อตอบโจทย์ Industry IoT ผ่านระบบ mobile application**

การประยุกต์ใช้ CYBLION จริงกับ Use Cases

CYBLION เป็นแพลตฟอร์มไอโอทีคลาวด์ที่ให้บริการคำนวณข้อมูลเข้ารหัสโดยไม่ถอดรหัสเพื่อความเป็นส่วนตัวของข้อมูล ได้ถูกทดสอบการใช้งานภาคสนาม ผ่านการนำไปใช้งานจริงในโรงงานอุตสาหกรรม 2 แห่ง ได้แก่

1. บริษัท ธนากรผลิตภัณฑ์น้ำมันพืช จำกัด (TVOP) ใช้แพลตฟอร์ม CYBLION สำหรับตรวจวัดค่าระดับของน้ำมันในไซโลน้ำมันแบบเรียลไทม์ จำนวน 2 ไซโล เพื่อแก้ปัญหาข้อกังวลข้อมูลปริมาณการผลิตน้ำมันของบริษัทรั่วไหลไปสู่บุคคลภายนอกในขณะที่บริษัทต้องการประเมินสถานการณ์การซื้อขายน้ำมันแบบเรียลไทม์ การใช้บริการไอโอทีคลาวด์แบบเดิมๆ ไม่ปลอดภัยอีกต่อไป ทั้งยังต้องเผชิญกับข่าวการรั่วไหลของข้อมูลบนคลาวด์สาธารณะจากการโดนแฮกเกอร์โจมตี หรือต้องเผชิญกับเบี้ยประกันภัยไซเบอร์ที่แพงขึ้นเนื่องจากความเสี่ยงของข้อมูลรั่วไหล และได้รับผลกระทบจากคู่แข่งทางการค้านำข้อมูลเหล่านั้นไปใช้ประโยชน์ การนำ CYBLION ไปใช้งานของบริษัท TVOP ในครั้งนี้เป็นบททดสอบทั้งความเป็นไปได้ของการนำเทคโนโลยี PET มาใช้งานจริง และการปกป้องความเป็นส่วนตัวของข้อมูลได้จริง พร้อมทั้งทดสอบประสิทธิภาพของการส่งข้อมูลไอโอทีแบบเข้ารหัสด้วยเทคนิคโฮโมมอร์ฟิกด้วยระบบการสื่อสารไร้สาย 5G ทั้งนี้ นักวิจัยได้เปรียบเทียบการใช้งานแพลตฟอร์ม CYBLION กับแพลตฟอร์มที่ให้บริการไอโอทีคลาวด์แบบไม่เข้ารหัสข้อมูลเพื่อประเมินความถูกต้องของข้อมูลภายหลังการคำนวณและแสดงผลข้อมูลที่ถอดรหัสแล้วบน Mobile Application

2. บริษัท เดอะ เพ็ท จำกัด ใช้ทดสอบแพลตฟอร์ม CYBLION สำหรับระบบตรวจสอบอุณหภูมิและความชื้นของระบบในโรงงาน โดยซอฟต์แวร์เข้ารหัสข้อมูลจะทำหน้าที่เข้ารหัสข้อมูลก่อนการส่งข้อมูลอุณหภูมิและความชื้น ก่อนส่งผ่านการสื่อสารไร้สาย WiFi ออกสู่ Internet ไปยัง CYBLION Cloud Platform โดยวิศวกรของโรงงานเป็นผู้สร้างสูตรการคำนวณ Due point ที่ใช้ข้อมูลอุณหภูมิและความชื้น ซึ่งผลของการคำนวณเป็นเงื่อนไข

เพื่อใช้ในการสั่งการให้เครื่องมือที่ต้องการควบคุมหยุดการทำงาน ชะลอการทำงาน หรือให้ผู้เกี่ยวข้องเข้าบำรุงรักษาก่อนเกิดความเสียหาย **ซึ่งจุดเด่นของการใช้งาน** แพลตฟอร์ม CYBLION อีกประการหนึ่งคือ การปรับเปลี่ยนสูตรการคำนวณสามารถทำได้บนคลาวด์โดยไม่กระทบกับระบบการทำงานเดิม ซึ่งแตกต่างจากวิธีการสร้างสูตรการคำนวณบน Edge computing ที่ทางโรงงานใช้อยู่เดิม ซึ่งการปรับเปลี่ยนสูตรคำนวณนั้นจะทำให้การทำงานของระบบหยุดชะงัก

โดยสรุปผลแล้ว แพลตฟอร์ม CYBLION สามารถใช้งานได้และข้อมูลแสดงผลถูกต้องผ่าน Mobile Application สามารถพัฒนาจากต้นแบบห้องปฏิบัติการเป็นต้นแบบภาคสนามที่มีการทดสอบใช้งานจริง จากนั้นทีมวิจัยได้เผยแพร่ผลการทดสอบการใช้งานแพลตฟอร์มไปยังกลุ่มผู้ใช้งานเป้าหมายจำนวนกว่า 60 คน ผ่านการจัดอบรมเชิงปฏิบัติการและการระดมความคิดเห็น โดยผู้เข้ารับการอบรมได้ให้คำแนะนำติชมและข้อเสนอแนะในการใช้งานแพลตฟอร์มที่พัฒนาขึ้น ซึ่งมีประโยชน์ต่อการนำไปปรับปรุงและพัฒนาแพลตฟอร์มเพื่อการใช้งานต่อไป ภายหลังการจัดอบรมและเผยแพร่องค์ความรู้ในเชิงวิชาการและการใช้งานแพลตฟอร์มก่อให้เกิดการเรียนรู้และตระหนักถึงความสำคัญของความปลอดภัยและความเป็นส่วนตัวของข้อมูลไอโอทีในโรงงานอุตสาหกรรมแก่กลุ่มเป้าหมาย

ทิศทางในอนาคตของ “PET”

นอกจากประโยชน์ในภาคอุตสาหกรรม จากตัวอย่างข้างต้น อนาคตการประยุกต์ใช้เทคโนโลยี PET ช่วยให้การบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลกลายเป็นเรื่องรอง โดยไม่ต้องบังคับให้ผู้ใช้บริการรับความยินยอมผ่านกระดาษ (consent form) อีกต่อไป แต่ทำให้การคุ้มครองข้อมูลส่วนบุคคลเป็นเรื่องหลัก ด้วยการใช้เทคโนโลยี PET มาทดแทนการใช้กระดาษหรือระบบ consent

เทคโนโลยี PET จะมีบทบาทมากขึ้นในทุกๆ application ที่ข้อมูลมีมูลค่า มีความสำคัญ และสร้างผลกระทบต่อสังคมในวงกว้าง ผู้คนจะตระหนักถึงการแชร์ข้อมูลสาธารณะมากยิ่งขึ้น และหาก application นั้นๆ ไม่ได้รองรับการคุ้มครองความปลอดภัยและความเป็นส่วนตัวของข้อมูลจะทำให้ความนิยมในการใช้ application

นั้นจะน้อยลง โดยเฉพาะอย่างยิ่งการมาของ AI ไม่ว่าจะเป็น ChatGPT หรือแม้กระทั่ง Gemini หรือ Perplexity ที่การแชร์ข้อมูลลงบน Platform ดังกล่าว เป็นการสูญเสียความเป็นส่วนตัวของข้อมูลหรือไม่ AI เหล่านี้จะสามารถ Clone ตัวตนของบุคคลต่างๆ ได้โดยไม่ได้รับการยินยอมหรือไม่ คำถามนี้ ควรมีคำตอบในเร็ว ๆ นี้

บทความโดย

ดร.กลิกา สุขสมบูรณ์	ทีมวิจัยระบบไซเบอร์-กายภาพ (CPS)	เนคเทค
ดร.จิรพรรณ เชาวนพงษ์	ฝ่ายพัฒนาเครือข่ายเชิงกลยุทธ์และประเมินผล (SPE)	เนคเทค